

HP 1/8 G2 Tape Autoloader and MSL Tape Library Encryption Kit Getting Started

Abstract

The HP 1/8 G2 Tape Autoloader and MSL Tape Library Encryption Kit may be used with HP StoreEver 1/8 G2 Tape Autoloaders, and MSL2024, MSL4048, MSL6480, MSL8048, and MSL8096 Tape Libraries with LTO-4 or later generation tape drives. It is not compatible with MSL6000 Tape Libraries.



© Copyright 2010, 2013 Hewlett-Packard Development Company, L.P.
Printed in the US

HP Part Number: AM495-96030
Published: June 2013
Edition: Third



CAUTION: The key server token protects access to the encryption keys with a personal identification number (PIN). If you lose the PIN, you will **NOT** be able to restore data from your encrypted tapes. Neither you nor HP can recover a lost PIN. Keep a copy of the PIN in a safe place.

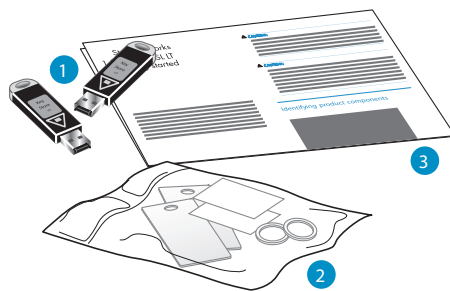
CAUTION: The encryption kit includes two key server tokens. If one token is lost or damaged, you will need the second token and the encryption key backup file to restore data from your encrypted tapes. HP recommends that you keep the second token in a safe place. When you create new keys, HP recommends that you keep a backup of the encryption keys in a safe place. Neither you nor HP can generate the encryption key for a tape. You will need a token, your encryption key backup file, and the token PIN to access your encrypted data.

The encryption kit provides secure storage for encryption keys and access to the encryption capability of the LTO-4 and later generation tape drives without requiring encryption support in the backup application. The encryption kit is designed to be used with manual processes for tracking the correlation between tape cartridges and tokens. To restore data from an encrypted tape cartridge, you must know which token has the encryption key for the tape cartridge.

For more information about encryption, developing security processes associated with the encryption kit, and operation of the encryption kit, download the *HP 1/8 G2 Tape Autoloader and MSL Tape Library Encryption Kit User Guide* from the HP website:

1. Browse to <http://www.hp.com/support/tape>.
2. In the **Tape Storage** section, select **Tape Libraries**.
3. Select **HP StoreEver MSL Tape Libraries**.
4. In the **Resources for HP StoreEver MSL Tape Libraries** section, select **Manuals**.
5. In the **User guide** section, select **HP 1/8 G2 Tape Autoloader and MSL Tape Library Encryption Kit User Guide**.

1 Identifying product components



1. Two key server tokens
2. Accessory bag of token ID cards and holders
3. Product documentation

2 Preparing the autoloader or library

Log in to the remote management interface

The key server token and autoloader or library encryption capabilities can only be configured from the web-based remote management interface (RMI). Log into the RMI as the administrator user.

If you have not used the RMI on this autoloader or library in the past, you must configure the network on the autoloader or library before continuing.

See the getting started guide that came with the autoloader or library, or the device user guide for instructions on configuring the network and using the RMI. You can find these documents on the HP website at <http://www.hp.com/support/manuals>.

Verify your autoloader or library firmware version

MSL6480

All MSL6480 firmware versions support the encryption kit.

Autoloader and other libraries



If you see the **Configuration: Security** tab in the RMI, the firmware supports the encryption kit. If this tab is

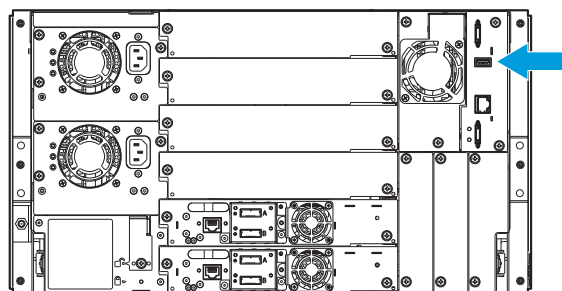
missing, update the autoloader or library firmware to the current version.

You can download autoloader or library firmware files from the HP Support website at <http://www.hp.com/support>.

Locate the USB port

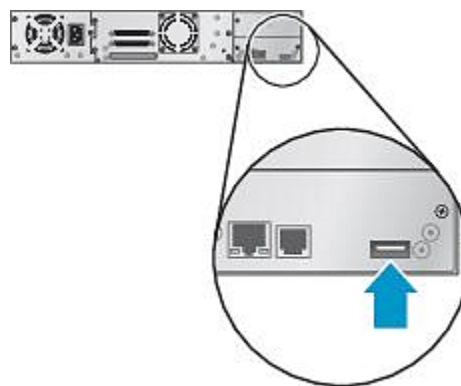
Locate the USB port on the back panel of the autoloader or library.

MSL6480



NOTE: Only the rear USB port on the MSL6480 is used for the encryption kit token.

Autoloader and other libraries



11868

If the USB port is covered with silver tape, remove the tape.

3 Preparing the key server tokens

As part of your security process, you will need to track each key server token, along with information associated with the token, as required by your security policy. If you do not have a security policy that specifies this information, download the *HP 1/8 G2 Tape Autoloader and MSL Tape Library Encryption Kit User Guide* from <http://www.hp.com/support/tape> for information about creating your encryption key management processes. HP recommends that you track at least:

- Token name
- Whether this token is a backup of another token
- Date range token was used for writing data
- The tape cartridges written with keys stored on the token. When possible, record the barcode label associated with the tape cartridge.
- Token backup file filename and password.

The encryption kit includes two methods of tracking the tokens. Choose the approach that works best for your security policy and organization. HP recommends that you use both approaches.

- Attached tag — The encryption kit includes a card and holder, which can be used to attach information to the token.
- Serial number — Each key server token has a unique serial number. You can use the serial number to identify the key server token and correlate the tape cartridges written with keys on the token.

- ❗ **IMPORTANT:** HP recommends that you maintain a record of the tape cartridges that are written with encryption keys on the key server token. When restoring the data from an encrypted tape, you will need to use the key server token containing the encryption key for that tape. The name of the key server token is not stored on the tape and the name of the tape is not stored on the key server token. If you do not know which token contains the key for a tape, you may need to try all of your key server tokens when restoring data from an encrypted tape. Each key server token can contain a maximum of 100 keys.

To use the attached tags to identify the tokens:

1. Write the token identification information on the paper cards.
2. Insert each card into a holder.

3. Attach the holders to the tokens.
4. Track the tape cartridges that are written with keys stored on the token and keep a copy of this record in a secure location.

To use the serial numbers to identify the tokens:

- Record the token identification information and tape cartridges that are written with keys stored on the token, and keep a copy of the record in a secure location.

💡 **TIP:** The serial number is on the bottom of the token when the token is in the autoloader or library, making it difficult to see. You can find the token serial number and firmware version from the RMI **Status: Security** screen or the MSL6480 home screen.

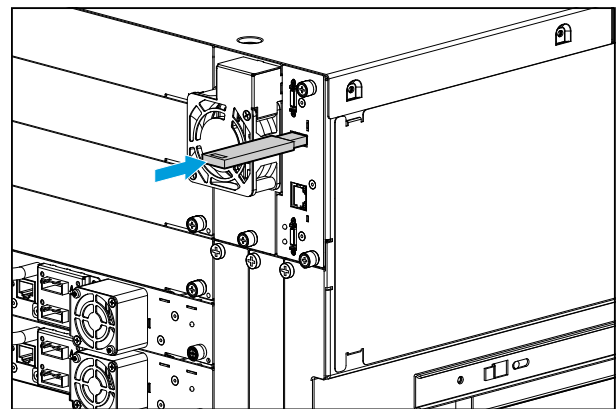
4 Configuring encryption

In this section, you will configure the name and personal information number (PIN) for the key server token and configure encryption on the autoloader or library.

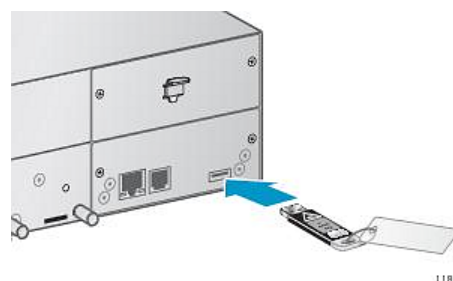
Insert the key server token

Insert the key server token in the USB port on the back panel of the autoloader or library.

MSL6480



Autoloader and other libraries



Enter the PIN

When the key server token is inserted, the autoloader or library will recognize it as a new token and display a dialog on the RMI requesting that you enter a PIN. The new PIN must be between 8 and 16 characters long and contain at least one capital letter, at least one lower case letter, and at least two digits. Follow the directions in the dialog to enter your PIN.

If too many incorrect PIN entries are attempted, the token must be removed and reinserted to attempt additional PIN entries.

Store a copy of the PIN in a secure location.

CAUTION: The key server token protects the encryption keys with a personal identification number (PIN). If you lose the PIN, you will not be able to restore data from your encrypted tapes. Neither you nor HP can recover a lost PIN. Keep a copy of the PIN in a safe place.

Configure the encryption mode and features

MSL6480

Pin Management

Change PIN

Enter Current PIN

Enter New PIN

(The PIN must be at least 8 and max 16 characters and long, contain at least one capital letter, one lower case letter and at least two digits. For more information about PIN formats and compatibility please read the Help page)

Repeat new PIN:

Submit

Change Token name

New Token Name

Submit

From the MSL6480 **Configuration > Encryption > USB — MSL Encryption Kit** screen Pin Management area you can change the PIN or token name.

Autoloader and other libraries

IdentityStatusConfigurationOperationsSupport

SystemSecurityDriveNetworkNetwork ManagementPasswordDate/Time

LogAlertsSave/Restore

Security Configuration

Encryption enabled

Automatic key generation policy

Token Name (maximum 128 characters)

Manually enter decryption key

Monday

At

8

:

0

Every

4

Weeks

Enabled

Add

Warning: This function is rarely used. Please read the Help page for more information before clicking Add.

Submit

Refresh

From the **Configuration: Security** page you can enter the name of the token, enable or disable encryption for the autoloader or library, and enable the autoloader or library to automatically generate new keys. If your library has multiple partitions, you can enable or disable encryption for each partition that contains an LTO-4 or later generation tape drive. Only one encryption key is used at a time to write tape cartridges and the same encryption key is used by all tape drives in the library.

Enter the name of the token in the **Token Name** field. By default, you must generate new keys manually. Optionally, you can enable **Automatic key generation** to have the autoloader or library to automatically generate a new key periodically. Set the generation time and period in accordance with your security policy. Once a token contains 100 keys you will need to obtain another token. Keys can never be deleted from the token.

Enable encryption for the autoloader or library, or for one or more partitions that contain an LTO-4 or later generation tape drive.

Click **Submit**.

NOTE: The library uses the same write encryption key (the Current key) for all logical libraries or partitions with encryption enabled. If the autoloader or library is writing an encrypted tape when you change the security configuration, the new configuration will take effect for the next tape loaded into an LTO-4 or later generation tape drive.

Seeding the new key server token

When transitioning from a full token to a new token, you can copy the highest numbered keys from the full token to the new token to enable read operations from tapes written with keys on the full token.

Keys are typically stored in the order that they were created. The new token has room for 100 keys. The more keys that are copied from the full token, the fewer keys can be created on the new token in the future.

1. Verify that no backup operations are in progress.
2. Log into the RMI **Configuration: Security** page or MSL6480 **Configuration > Encryption > USB — MSL Encryption Kit** screen.
3. Insert the full token into the USB port on the back of the autoloader or library, and enter the PIN.

If the **Number of Keys to Backup** option is not visible, you must back up all keys on the token to a file before creating a file with just some of the keys. To back up the full token, see [“Backing up the token data”](#) (page 5).

4. In the **Back up Token to File** pane, enter a password, which will be used to secure the data file on the computer, in both fields. The second password entry ensures that the password was typed correctly.
5. Click **Submit Token Backup File Password**.
6. In the **Number of Keys to Backup** field, select the number of keys to copy onto the new token. The highest-numbered keys, which are normally the most recent, will be copied. For example, if the token has 100 keys and you select 3, keys 98, 99, and 100 will be copied.
7. Click **Save**. The RMI will prompt you for the location to save the file. Follow the instructions in the RMI.
8. Insert the new token into the USB port of the autoloader or library, and enter the PIN.
9. Enter the password used to create the token backup file. Click **Submit Token Restore File Password**.
10. Browse to the location of the token backup file containing the seed keys. Click **Restore**. (The **Browse** button will be active after the token restore file password is submitted.)
11. If you paused write operations at the beginning of the procedure, you can resume them.

Backing up the token data

You can back up the keys on the token from the RMI, which requires the administrator password. During the token backup process, the autoloader or library will write the token information to a file in a secure format, which will be saved on the computer from which you are running the browser with the RMI. After the file is written, the information can be restored to a different token.

MSL6480

1. Navigate to the **Configuration > Encryption > USB — MSL Encryption Kit** screen.
2. Expand the **Key Management** section.
3. Enter a password, which will be used to secure the data file on the computer, in both fields. The second password entry ensures that the password was typed correctly.

The password must be at least 8 characters and no longer than 16 characters. The password must contain at least one lower case letter, one upper case letter, and at least two digits.

4. Click **Save**.

Autoloader and other libraries

1. Navigate to the **Configuration: Security** page.
2. In the **Back up Token to File** pane, enter a password, which will be used to secure the data file on the computer, in both fields. The second password entry ensures that the password was typed correctly.

The password must be at least 8 characters and no longer than 16 characters. The password must contain at least one lower case letter, one upper case letter, and at least two digits.

3. Click **Submit Token Backup File Password**.
4. Click **Save**. The RMI will prompt you for the location to save the file. Follow the instructions in the RMI.

After a power cycle

For increased security, the key server token's PIN is stored in volatile memory in the autoloader or library. Each time the autoloader or library is powered on, the PIN must be entered. The autoloader or library will display a warning message on the OCP and RMI, and send periodic SNMP and email events, if those options are enabled, until the PIN is entered. The autoloader or library will not read or write encrypted data until the PIN is entered.

⚠ CAUTION: If it is critical that the autoloader or library maintain encryption capability in the event of a power loss, HP recommends that you plug the autoloader or library's power cable into an uninterruptable power supply (UPS).

Viewing security status

MSL6480

The **Status > Security** screen displays the status of the key server token and drive encryption.

- **Key Server Token Status** — Identity of the key server token, if any, present in the rear USB port.
- **Drive Encryption Status** — Whether each drive is configured to encrypt data with the MSL Encryption Kit.

Autoloader and other libraries

The RMI **Status: Security** screen shows the encryption status for each of the tape drives, along with information about the key server token. When the **Key Server Token Status** is **Token backup required**, you should back up the keys to a file and store the file in a safe place.

Helpful websites

For other product information, see the following websites:

www.hp.com/go/ebs

www.hp.com/go/tape

www.hp.com/go/storage

www.hp.com/support

www.hp.com/support/mslg3tstree

www.hp.com/support/TapeTools

www.hp.com